WENDEROTH, LIND & PONACK, L.L.P.
2033 K Street, N.W., Suite 800
Washington, D.C. 20006

Telephone: (202)721-8218
Facsimile: (202)721-8250

FAX TRANSMISSION COVER SHEET

To: Examiner John B King

Fax Number: 571-270-8310

From: Andrew Dunlap (202-721-8218)

Date: February 20, 2009

TOTAL NUMBER OF PAGES TRANSMITTED, INCLUDING COVER SHEET 18

Message:

Examiner King, as previously discussed, I have attached a proposed amendment prepared by the Applicants for application no. 10/559,725. Our interview is scheduled for 2:00 pm on March 3, 2009. If you have any questions beforehand, feel free to contact me.

Best Regards,

Andrew Dunlap

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	**Confirmation No. 1837**
Noriko Yuichi FUTA et al.	:	Attorney Docket No. 2005_1849A
Serial No. 10/559,725	:	Group Art Unit 4148
Filed December 07, 2005	:	Examiner John B KING
ENCRYPTED COMMUNICATION SYSTEM	:	**Mail Stop: F.A.**

RESPONSE UNDER 37 C.F.R. § 1.116

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action of January 23, 2009, kindly amend the above-referenced U.S. patent application as follows:

AMENDMENTS TO THE CLAIMS

1. **(Currently Amended)** An encryption communication system for secret message communication, the encryption communication system comprising an encryption transmission apparatus and an encryption reception apparatus,

wherein the encryption transmission apparatus includes:

a storage unit that stores one message;

an encryption unit operable to perform an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption unit being equal to the number of times the encryption unit performs the encryption computation on the one message;

a computation unit operable to perform a one-way operation on the one message to generate a one comparison computation value; and

a transmission unit operable to transmit, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value, and

wherein the encryption reception apparatus includes:

a reception unit operable to receive, from the encryption transmission apparatus, the plurality of the encrypted messages and the one comparison computation value;

a decryption unit operable to perform a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the plurality of the encrypted messages to generate a plurality of decrypted messages, and a number of decrypted messages generated by the decryption unit being equal to the number of the encrypted messages generated from the one message by the encryption unit;

a computation unit operable to perform the one-way operation on each of the decrypted messages to generate a plurality of decryption computation values, a number of decryption values generated by the computation unit being equal to the number of the decrypted messages generated by the decryption unit; and

a judging unit operable to compare each of the decryption computation values with the one received comparison computation value,

wherein i) when at least one of the decryption computation values matches the one received comparison computation value, the judging unit outputs a decrypted message as a correct decrypted message, and ii) when none of the decryption computation values matches the one received comparison computation value, the judging unit determines that there is a decryption error.

2. (Previously Presented) The encryption communication system of claim 1,

wherein the encryption computation used by the encryption unit conforms to NTRU cryptosystem, and

wherein the decryption computation used by the decryption unit conforms to the NTRU cryptosystem.

3. (Currently Amended) An encryption transmission apparatus for secret message communication with an encryption reception apparatus, the encryption transmission apparatus comprising:

a storage unit that stores one message;

an encryption unit operable to perform an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption unit being equal to the number of times the encryption unit performs the encryption computation on the one message;

a computation unit operable to perform a one-way operation on the one message to generate a one comparison computation value; and

a transmission unit operable to transmit, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value.

4. (Previously Presented) The encryption transmission apparatus of claim 3, wherein the encryption unit comprises:

an encryption computation subunit operable to perform an invertible data conversion on the one message to generate a converted message, and perform an encryption algorithm on the converted message to generate one encrypted message; and

a repetition control subunit operable to control the encryption computation subunit to repeat the generation of the converted message and the generation of the one encrypted message, the generation of the converted message and the generation of the one encrypted message being repeated the plural number of times the encryption unit performs the encryption computation on the one message to generate the plurality of encrypted message.

5. (Previously Presented) The encryption transmission apparatus of claim 4, wherein the encryption computation subunit generates a random number of a fixed length, and generates the converted one message by adding the random number to the one message.

6. (Previously Presented) The encryption transmission apparatus of claim 5, wherein the encryption algorithm used by the encryption computation subunit on the converted message conforms to NTRU cryptosystem.

7. (Currently Amended) An encryption reception apparatus for secret message communication with an encryption transmission apparatus, the encryption transmission apparatus storing one message, performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message by the encryption unit being equal to the number of times the encryption unit performs the encryption computation on the one ~~message~~ message, performing a one-way operation on the one message to generate a comparison computation value, and transmitting, to the encryption reception apparatus, the plurality of encrypted messages and the comparison computation value, the encryption reception apparatus comprising:

a reception unit operable to receive, from the encryption transmission apparatus, the plurality of encrypted messages and the one comparison computation value;

a decryption unit operable to perform a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the plurality of the encrypted messages to generate a plurality of decrypted messages, and a number of decrypted messages generated by the decryption unit being equal to the number of the encrypted messages generated from the one message by the encryption transmission apparatus

a computation unit operable to perform the one-way operation on each of the decrypted messages to generate a plurality of decryption computation values, a number of decryption values generated by the computation unit being equal to the number of the decrypted messages generated by the decryption unit;

a judging unit operable to compare each of the decryption computation values with the one received comparison computation value,

wherein i) when at least one of the plurality of the decryption computation values matches the received comparison computation value, the judging unit outputs a decrypted message as a correct decrypted message, and ii) when none of the decryption computation values matches the one received comparison computation value, the judging unit determines that there is a decryption error.

8. **(Previously Presented)** The encryption reception apparatus of claim 7,

wherein the encryption transmission apparatus performs an invertible data conversion on the one message to generate a converted message, and perform an encryption algorithm on the converted message to generate one encrypted message, and repeats the generation of the converted message and the generation of the one encrypted message being repeated the plural number of times the encryption unit performs the encryption computation on the one message to generate the plurality of encrypted messages, and

wherein the decryption unit comprises:

a decryption computation subunit operable to perform a decryption algorithm to

corresponding to the encryption algorithm, on one of the plurality of the encrypted messages to generate one decrypted text, and perform an inverse conversion of the invertible data conversion on the one decrypted text to generate one decrypted message; and

a repetition control subunit operable to control the decryption computation subunit to repeat the generation of the one decrypted content and the generation of the one decrypted message, the generation of the one decrypted content and the generation of the one decrypted message being repeated the plural number of times the decryption unit performs the decryption computation to generate the plurality of the decrypted messages being equal in number to the number of the encrypted messages generated from the one message by the encryption unit.

9. (Previously Presented) The encryption reception apparatus of claim 8,

wherein the encryption transmission apparatus generates a random number of a fixed length, and generates the converted one message by adding the random number to the one message, and

wherein the decryption computation subunit generates the decrypted the one message by removing the random number of the fixed length from the one decrypted text.

10. (Previously Presented) The encryption reception apparatus of claim 9,

wherein the encryption algorithm used by the encryption transmission apparatus conforms to NTRU cryptosystem, and

wherein the decryption algorithm used by the decryption computation subunit conforms to the NTRU cryptosystem.

11. (Currently Amended) An encryption transmission method used in an encryption transmission apparatus, the encryption transmission apparatus storing one message and transmitting the one message in secrecy to an encryption reception apparatus, the encryption transmission method comprising:

performing an encryption computation on the one message a plural number of times to

generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the performing of the encryption computation being equal to the number of times the performing of the encryption computation performs the encryption computation on the one message;

performing a one-way operation on the one message to generate a one comparison computation value; and

transmitting, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value.

12. (Currently Amended) A computer-readable recording medium having an encryption transmission program recorded thereon, the encryption transmission program being used in an encryption transmission apparatus, the encryption transmission apparatus storing one message and transmitting the message in secrecy to an encryption reception apparatus, the encryption transmission program causing the encryption transmission apparatus to execute a method comprising:

performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the performing of the encryption computation being equal to the number of times the performing of the encryption computation performs the encryption computation on the one message;

performing a one-way operation on the one message to generate a one comparison computation value; and

transmitting, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value.

13. (Canceled).

14. (Currently Amended) An encryption reception method used in an encryption

reception apparatus, the encryption reception apparatus receiving a message from an encryption transmission apparatus in secrecy, the encryption transmission apparatus storing the one message, performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal to the number of times the encryption transmission apparatus performs the encryption computation on the one message, performing a one-way operation on the one message to generate a one comparison computation value, and transmitting, to the encryption reception apparatus, the plurality of encrypted messages and the one comparison computation value, the encryption reception method comprising:

receiving, from the encryption transmission apparatus, the plurality of encrypted messages and the comparison computation value;

performing a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the encrypted messages to generate a plurality of decrypted messages, and a number of decrypted messages generated by the performing of the decryption computation being equal to the number of the encrypted messages generated from the one message by the encryption transmission apparatus;

performing the one-way operation on each of the decrypted messages to generate a plurality of decryption computation values, a number of decryption computation values generated by the performing of the one-way operation being equal to the number of the decrypted messages generated by the performing of the decryption computation;

comparing each of the decryption computation values with the received comparison computation value;

outputting a decrypted message that corresponds to a decryption computation value that the matches the one received comparison computation value, based on the comparing, as a correct decrypted message when at least one of the plurality of the decryption computation values matches the one received comparison computation value; and

determining that there is a decryption error when, as a result of the comparing, none of

the plurality of the decryption computation values matches the one received comparison computation value.

15. (Currently Amended) A computer-readable recording medium having an encryption reception program recorded thereon, the encryption reception program being used in an encryption reception apparatus, the encryption reception apparatus receiving a message from an encryption transmission apparatus in secrecy, the encryption transmission apparatus storing the one message, performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal to the number of times the encryption transmission apparatus performs the encryption computation on the one message, performing a one-way operation on the one message to generate a one comparison computation value, and transmitting, to the encryption reception apparatus, the plurality of encrypted messages and the one comparison computation value, the encryption reception program comprising:

receiving, from the encryption transmission apparatus, the plurality of encrypted messages and the comparison computation value;

performing a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the encrypted messages to generate a plurality of decrypted messages, and a number of decrypted messages generated by the performing of the decryption computation being equal to the number of the encrypted messages generated from the one message by the encryption transmission apparatus;

performing the one-way operation on each of the decrypted messages to generate a plurality of decryption computation values, a number of decryption computation values generated by the performing of the one-way operation being equal to the number of the decrypted messages generated by the performing of the decryption computation;

comparing each of the decryption computation values with the received comparison computation value;

outputting a decrypted message that corresponds to a decryption computation value that the matches the one received comparison computation value, based on the comparing, as a correct decrypted message when at least one of the plurality of the decryption computation values matches the one received comparison computation value; and

determining that there is a decryption error when, as a result of the comparing, none of the plurality of the decryption computation values matches the one received comparison computation value.

16. (Canceled).

REMARKS

Upon entry of this amendment, claims 1, 3, 7, 11-12 and 14-15 will have been amended for consideration by the Examiner. Thus, claims 1-12, and 14-15 currently remains pending. In this regard, Applicants note that the amended claims merely clarify the subject matter recited the rejected claims, but do not narrow the scope of the claims. No new matter has been added.

I. Claim Objection

Claim 7 is objected to because of the informalities. By the present amendment, Applicants have amended claim 7 to replace the misspelled term "mesasage" with the correct term "message". Thus, Applicants respectfully request that the Examiner withdraw the objection.

II. Claim Rejection under 35 U.S.C. § 103(a)

Claims 1-2, 7-10, and 14-15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Yamamichi et al. (U.S. Patent Publication No. 2002/0116612) in view of Olson et al. (US Pre-grant Publication 2003/0226007).

Independent calim 1 recites the features of an encryption communication system for secret message communication. The system includes an encryption transmission apparatus and an encryption reception apparatus. The encryption transmission apparatus includes: a storage unit that stores one message; an encryption unit operable to perform an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message (a number of encrypted messages generated from the one message by the encryption unit being equal to the number of times the encryption unit performs the encryption computation on the one message); a computation unit operable to perform a one-way operation on the one message to generate one comparison computation value; and a transmission unit operable to transmit, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value. The encryption reception apparatus includes: a reception unit operable to receive, from the encryption transmission apparatus, the

plurality of the encrypted messages and the one comparison computation value; a decryption unit operable to perform a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the plurality of the encrypted messages to generate a plurality of decrypted messages (a number of decrypted messages generated by the decryption unit being equal to the number of the encrypted messages generated from the one message by the encryption unit); a computation unit operable to perform the one-way operation on each of the decrypted messages to generate a plurality of decryption computation values, a number of decryption values generated by the computation unit being equal to the number of the decrypted messages generated by the decryption unit; and a judging unit operable to compare each of the decryption computation values with the one received comparison computation value, wherein i) when at least one of the decryption computation values matches the one received comparison computation value, the judging unit outputs a decrypted message as a correct decrypted message, and ii) when none of the decryption computation values matches the one received comparison computation value, the judging unit determines that there is a decryption error.

Independent claim 3 recites a related encryption transmission apparatus, and independent claim 7 recites a related encryption reception apparatus. Independent claim 11 recites a method related to independent claim 3, and independent claim 12 recites a computer program related to independent claim 3. Independent claim 14 recites a method related to independent claim 7, and independent claim 15 recites a computer program related to independent claim 7.

Applicants respectfully submit that the applied prior art references do not teach or suggest the above-noted combination of features recited in amended independent claims 1, 3, 7, 11-12 and 14-15.

Regarding the Yamamichi reference, Applicants note that this reference discloses a system including a transmission apparatus and a reception apparatus. The transmission apparatus performs a one-way operation on a plaintext to generate a first value, generates first additional information, performs an invertible operation on the plaintext and the first additional information to generate connected information, encrypts the connected information according to

an encryption algorithm to generate ciphertext, and transmits the first value and the ciphertext to the reception apparatus.

Further, Yamamichi teaches that the reception apparatus receives, from the transmission apparatus, the first value and the ciphertext, generates a second additional information identical to the first additional information, decrypts the ciphertext according to a decryption algorithm, which is an inverse-conversion of the encryption algorithm, to generate the connected information, and decrypts the connected information and the second additional information according to an inverse operation of the invertible operation to generate decrypted text. Then, according to Yamamichi, the reception apparatus receives performs the one-way operation on the decrypted text to generate second value, compares the first and the second values, and judges that the decrypted text is valid when the first value matches the second value.

However, according to Yamamichi, when a plain text is judged to be decrypted incorrectly, a receiving party can request the transmitting party to re-transmit the encrypted text to the receiving party and can obtain the encrypted text again. This means that, when an attacker transmits some dummy data to the receiving party, the attacker can checks whether the receiving party can request the attacker to re-transmit the encrypted text to the receiving party. When the receiving party did not request the attacker to re-transmit the encrypted text to the receiving party, the attacker can determines that the receiving party can correctly decrypt the dummy data that attacker has transmitted to the receiving party. In this case, the attacker can obtain a key for the cryptosystem, using the dummy data that attacker has transmitted to the receiving party. This means that the security cannot be protected for the cryptosystem (see page 3, lines 4-7 and page 4, lines 1-9 of the specification).

In contrast, according to the present invention, an encryption communication system includes an encryption transmission apparatus and an encryption reception apparatus. An encryption transmission apparatus i) performs an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption unit being equal to the number of times the encryption unit performs the encryption computation on the one

message, ii) performs a one-way operation on the one message to generate one comparison computation value, and iii) transmits, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value. The encryption reception apparatus i) receives, from the encryption transmission apparatus, the plurality of the encrypted messages and the one comparison computation value, ii) performs a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the plurality of the encrypted messages to generate a plurality of decrypted messages, and a number of decrypted messages generated by the decryption unit being equal to the number of the encrypted messages generated from the one message by the encryption unit, iii) performs the one-way operation on each of the decrypted messages to generate a plurality of decryption computation values, a number of decryption values generated by the computation unit being equal to the number of the decrypted messages generated by the decryption unit, and iv) compares each of the decryption computation values with the one received comparison computation value. Then, the encryption reception apparatus i) outputs a decrypted message as a correct decrypted message, when at least one of the decryption computation values matches the one received comparison computation value, the judging unit, and ii) determines that there is a decryption error, when none of the decryption computation values matches the one received comparison computation value.

According to the combinations of the above features recited in the present invention, the present invention can reduce a possibility that a decryption error occurs, and thus, can reduce opportunities that the receiving party requests the attacker to re-transmit the encrypted text to the receiving party. Therefore, the present invention can obtain an unpredictable result to avoid the attack using the request for re-transmitting the encrypted text to the receiving party.

However, Yamamichi fails to disclose at least a system in which an encryption transmission apparatus i) performs an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption unit being equal to the number of times the encryption unit performs the encryption computation on the one message,

and ii) performs a one-way operation on the one message to generate one comparison computation value, and iii) transmits, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value, as recited in independent claims 1, 3, 7, 11-12 and 14-15.

Rather, Yamamichi merely teaches that the transmission apparatus generates one piece of encrypted information from one plain text (see Figs.4 and 5 and paragraphs [0079] and [0108]-[0112], which explain the operation of the encrypting unit 105 identified in paragraphs [0070] and [0071], as identified by the Examiner). Thus, Yamamichi fails to disclose or suggest performing encryption computation on one message a plural number of times, and generating the encryption unit performs the computation on the one message, as required by independent claims 1, 3, 7, 11-12 and 14-15.

Yamamichi also fails to disclose at least a system in which an encryption reception apparatus i) receives, from the encryption transmission apparatus, the plurality of the encrypted messages and the one comparison computation value, ii) performs a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the plurality of the encrypted messages to generate a plurality of decrypted messages, and a number of decrypted messages generated by the decryption unit being equal to the number of the encrypted messages generated from the one message by the encryption unit, as recited in independent claim 1, 7, and 14-15.

Further, Yamamichi fails to disclose or suggest the encryption reception apparatus including a judging unit that compares each of the decryption computation values with the one received comparison computation value, wherein i) when at least one of the decryption computation values matches the one received comparison computation value, the judging unit outputs a decrypted message as a correct decrypted message, and ii) when none of the decryption computation values matches the one received comparison computation value, the judging unit determines that there is a decryption error, as recited in independent claim 1, 7, and 14-15.

Rather, Yamamichi merely teaches that the reception apparatus generates the one plain text from the one piece of encrypted information (Figs.6 and paragraphs [0115]-[0119]). Thus,

Yamamichi fails to disclose or suggest performing decryption computation corresponding to the encryption, on each of the encrypted messages, and generating a plurality of decrypted messages, the number of decrypted messages generated by the decryption unit being equal to the number of encrypted messages generated from the one message by the encryption unit, as recited in independent claim 1, 7, and 14-15.

Additionally, Yamamichi also does not include any disclosures regarding a reception apparatus that i) outputs a decrypted message as a correct decrypted message, when at least one of the decryption computation values matches the one received comparison computation value, and ii) determines that there is a decryption error, when none of the decryption computation values matches the one received comparison computation value, as recited in independent claim 1, 7, and 14-15.

Thus, Yamamichi increases a possibility that a decryption error occurs, and thus, increases opportunities that the receiving party requests the attacker to re-transmit the encrypted text to the receiving party. Therefore, Yamamichi cannot avoid the attack using the request for re-transmitting the encrypted text to the receiving party (see page 3, lines 4-7 and page 4, lines 1-9 of the specification).

Therefore, independent claims 1, 3, 7, 11-12 and 14-15 are clearly distinguished over the Yamamichi reference.

In setting forth the rejection, the Examiner relies on Olson regarding that which the Examiner admits is lacking in Yamamichi. However, the Examiner cites Olson by asserting "the judging unit outputs decrypted message as a correct decrypted message". Thus, Olson fails to disclose or suggest the above combinations of the features recited in the pending claims.

Therefore, Applicants submit that even if one attempted to combine the teaching of Yamamichi with Olson in the matter suggested by the Examiner, one would fail to arrive at the presently claimed invention, since neither Yamamichi nor Olson disclose or suggest the above combinations of the features recited in the pending claims.

Therefore, Applicants submit that the suggested combination of Yamamichi with Olson does not render the presently claimed invention obvious, and thus, respectfully request that the

U.S.C. § 103(a) rejection be withdrawn.

Accordingly, Applicants respectfully request reconsideration and withdrawal of the outstanding rejection and an indication of the allowability of all the claims pending in the present application in due course.

Therefore, Applicants respectfully submit that independent claims 1, 3, 7, 11, 12, 14 and 15 are patentable over the cited prior art. Claim 2 depends from independent claim 1, claims 4-6 depend from independent claim 3, claims 8-10 depend from independent claim 7, and thus claims 2, 4-6, and 8-10 are considered patentable at least by virtue of their dependency.

III. Conclusion

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance and an early notification thereof is earnestly requested. The Examiner is invited to contact the undersigned by telephone to resolve any remaining issues.

Respectfully submitted,

Yuichi FUTA et al.

By: _____
Andrew L. Dunlap
Registration No. 60,554
Attorney for Applicants

ALD/krg
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
February 13, 2009